$\mathcal{L}$attice Problems beyond Polynomial Time

Divesh Aggarwal

Huck Bennett

Zvika Brakerski

Sasha Golovnev

Rajendra Kumar

Zeyong Li

Spencer Peters

Noah Stephens-Davidowitz

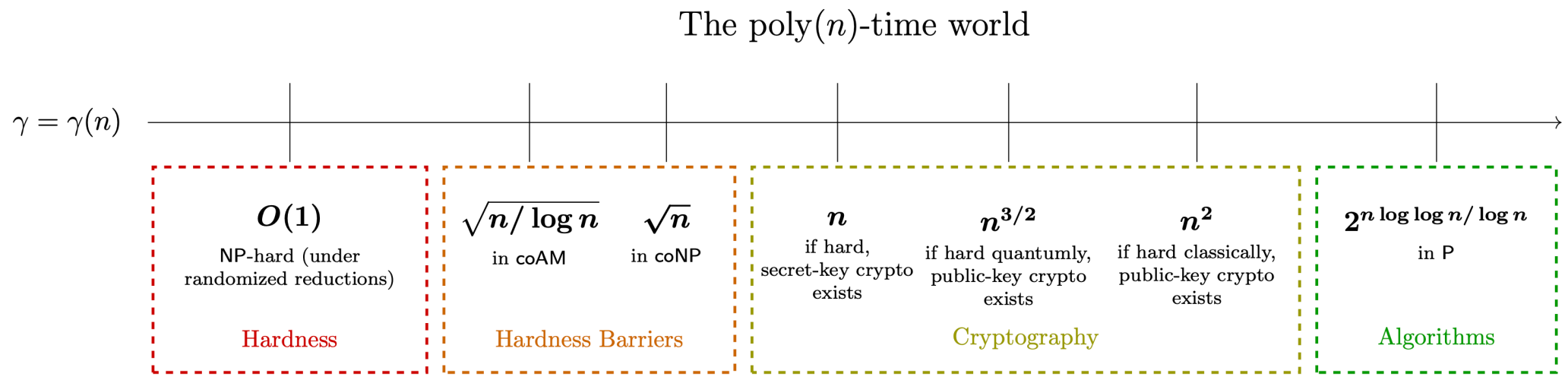
Vinod Vaikuntanathan

Organization

- Flipping the usual order!
- FIRST, an overview of results, so you have the big picture in mind
- THEN background, motivation, and implications

Overview

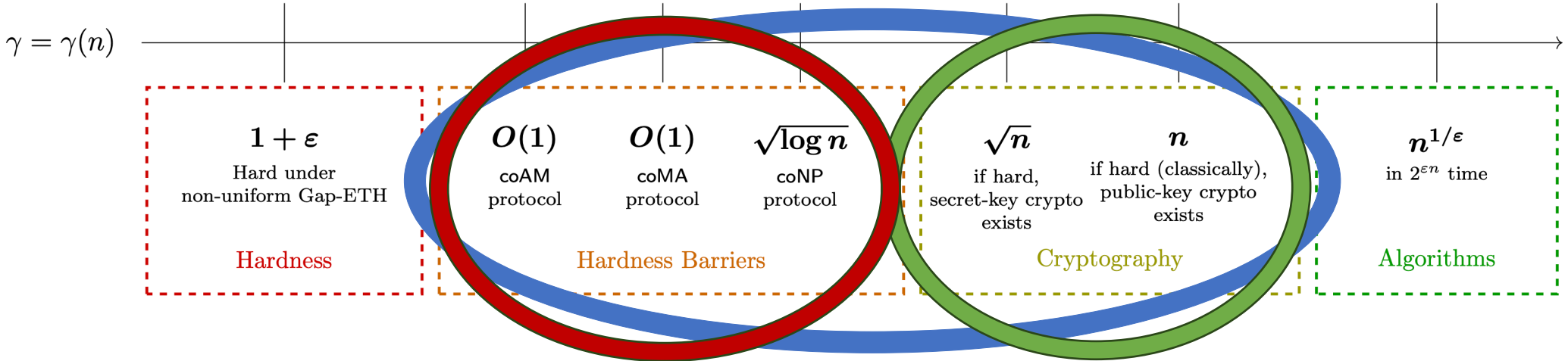
Approximating a certain important problem…



Barriers to proving exponential hardness from, for example, the Exponential Time Hypothesis ☹

Our work!

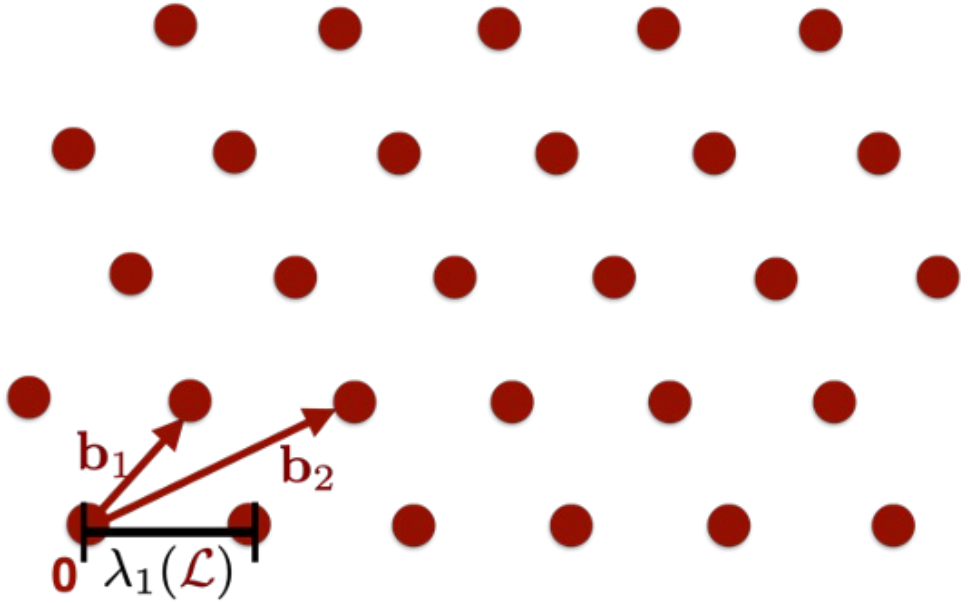
Better security guarantees! (Assuming **exponential** hardness, widely believed.)



Background

(What approximation problem are we talking about?!)

Lattices



- A *lattice* is a set of the form

$$\mathcal{L} = \{z_1\boldsymbol{b_1} + z_2\boldsymbol{b_2} + \cdots + z_n\boldsymbol{b_n} : z_i \in \mathbb{Z}\}$$

where $\boldsymbol{b_1}, \boldsymbol{b_2}, \ldots, \boldsymbol{b_n} \in \mathbb{R}^d$ are linearly independent.

- $\lambda_1(\mathcal{L}) := \min_{\boldsymbol{v}\in\mathcal{L},\boldsymbol{v}\neq 0} \| \boldsymbol{v} \|$. (The length of a shortest nonzero vector in $\mathcal{L}$.)

- The γ-approximate Shortest Vector Problem (γ-SVP): given a *basis* $\boldsymbol{B}$ for $\mathcal{L}$ and number r, decide whether

$$\lambda_1(\mathcal{L}) \leq r, \qquad \text{or} \qquad \lambda_1(\mathcal{L}) > \gamma \cdot r.$$

Lattice Cryptography

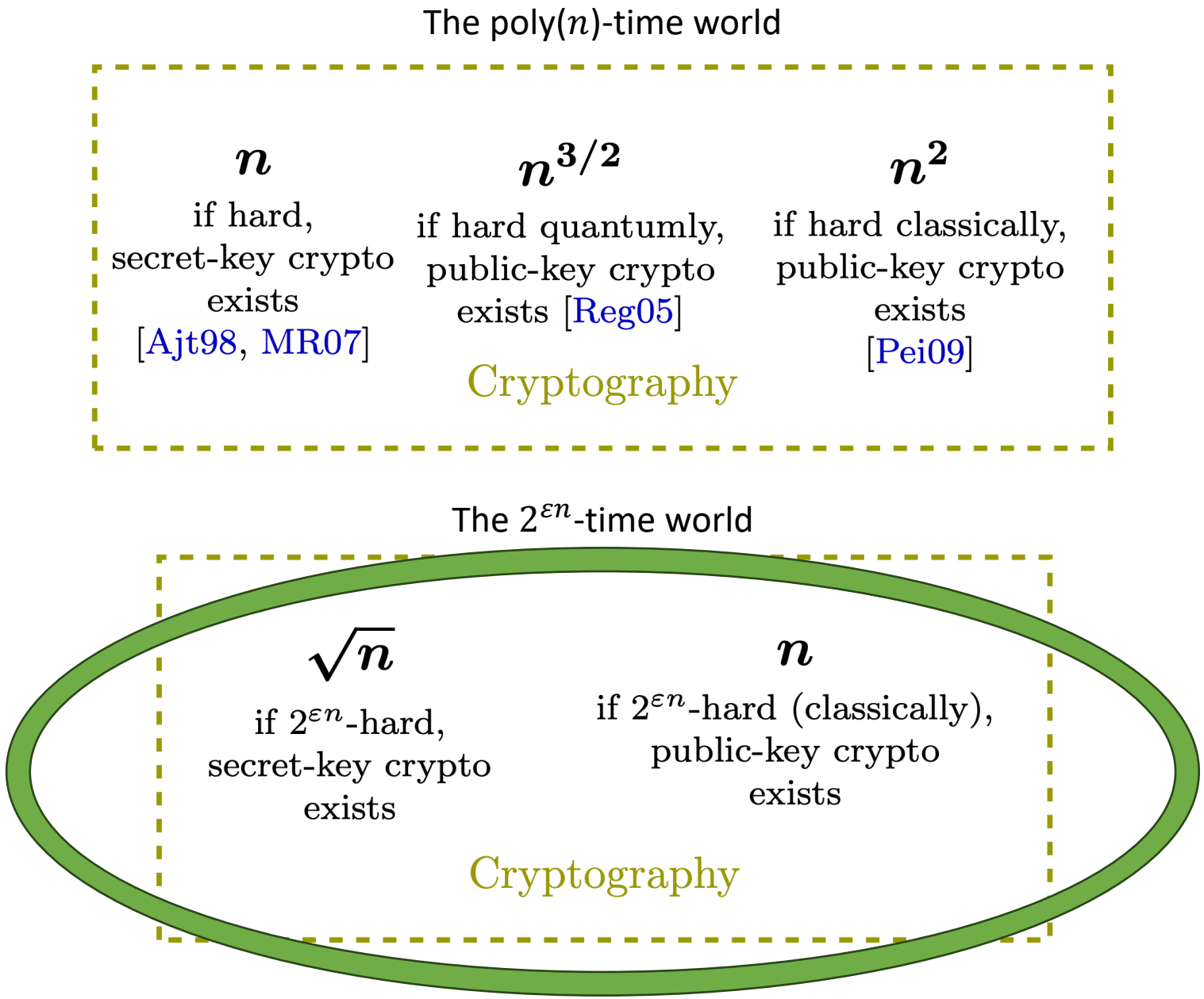
(or, why is SVP so important?)

- Cryptography that is
  - Believed post-quantum secure (and recently standardized by NIST for that reason [NIST22]).
  - Based on worst-case assumptions as opposed to average-case ones [Ajt96, Reg05, MR07, Pei09].
  - Enabling advanced constructions, most notably Fully Homomorphic Encryption (FHE) [Gen09, BV11].

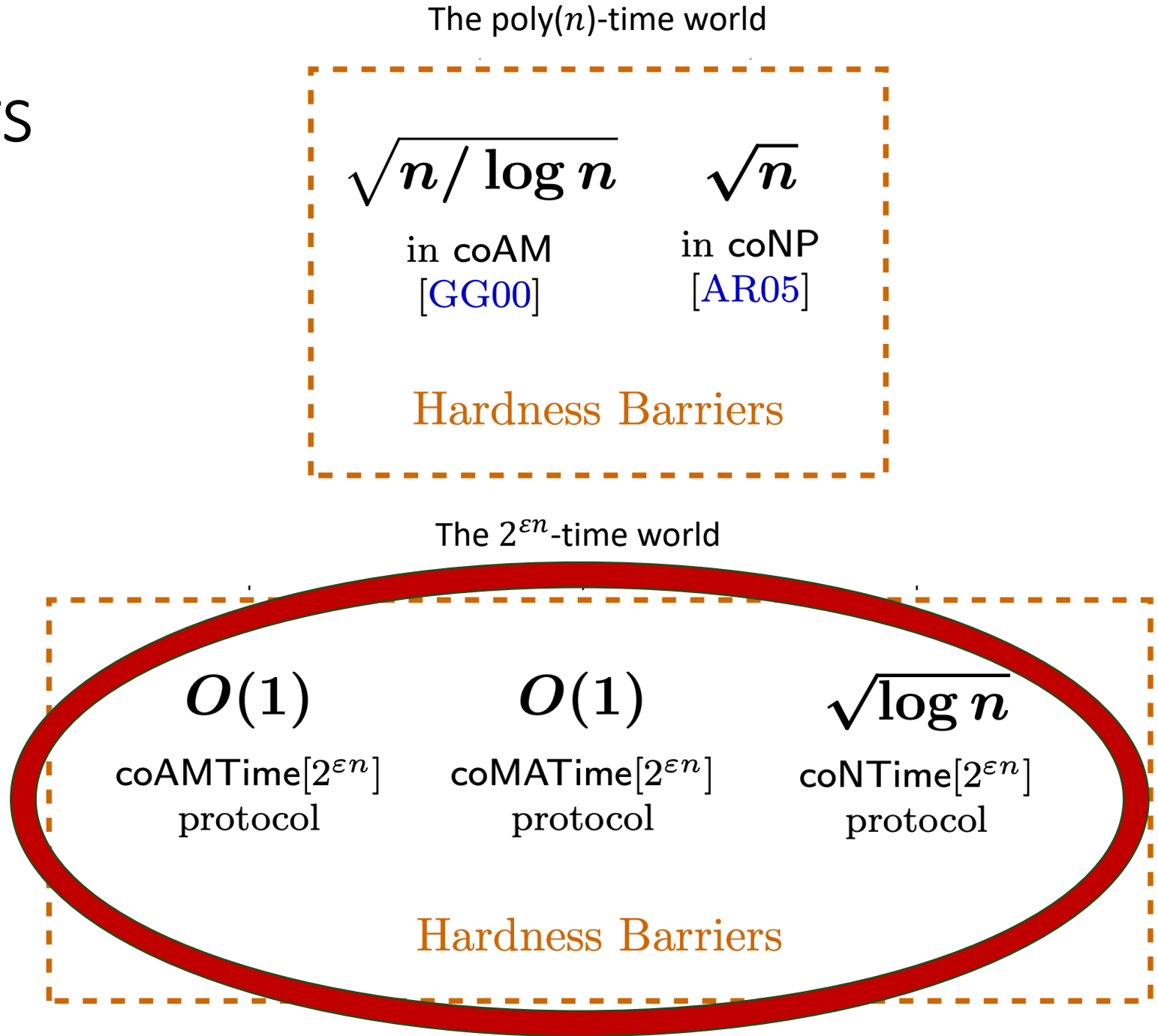
- Why “beyond Polynomial Time”?
  - Widely believed that the fastest algorithms for n^c-SVP run in time $2^{\Omega(\frac{n}{c})}$.
  - Assumed in setting parameters!
  - If we’re making this assumption in practice, we should make use of it in theory for better security guarantees.
  - We should also try to prove (conditional) exponential hardness.

Results and Implications

Security Guarantees

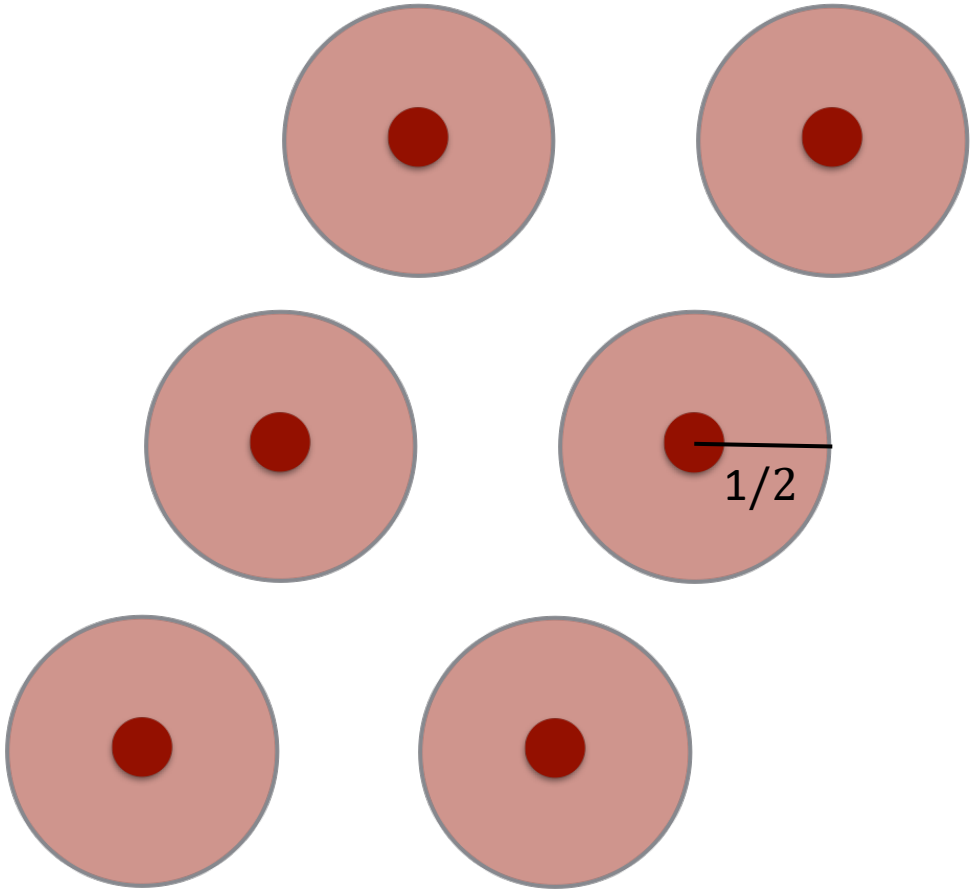


Hardness Barriers

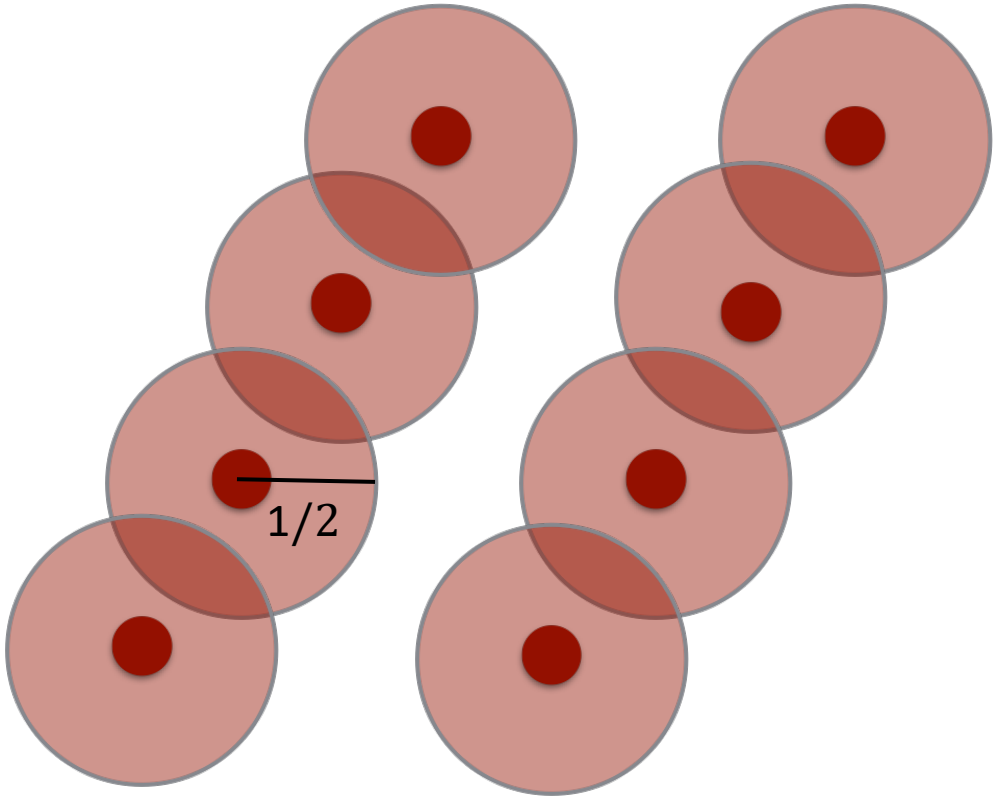


Example: coAM

Claim: $\sqrt{n/\log n}$-SVP $\in$ coAM



$\lambda_1(\mathcal{L}) > 1$ $\Rightarrow$ balls are disjoint.

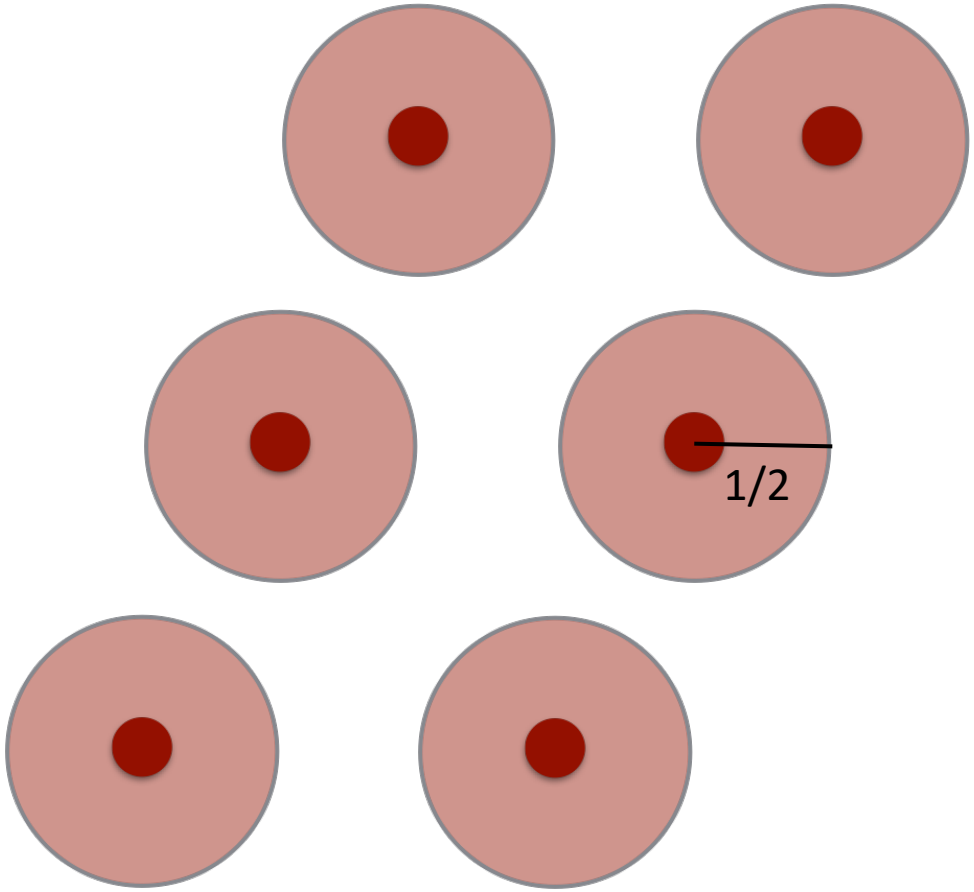


$\lambda_1(\mathcal{L}) \leq \sqrt{\frac{\log n}{n}}$ $\Rightarrow$ at least $1/\mathrm{poly}(n)$ fraction of each ball overlaps.

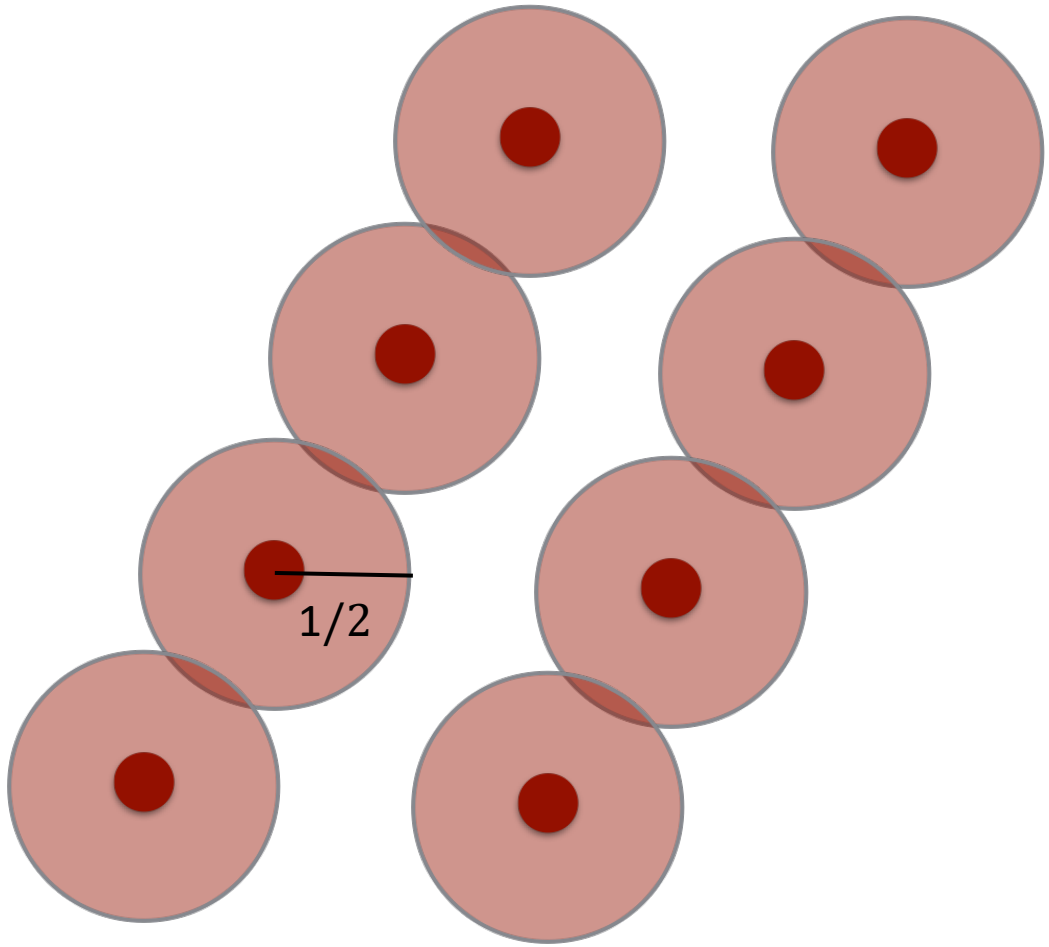
Private-coin protocol. Can be made public-coin (true coAM) with standard tricks.

Example: coAM

Claim: $O_\varepsilon(1)$-SVP $\in \mathrm{coAMTime}[2^{\varepsilon n}]$



$\lambda_1(L) > 1 \Rightarrow$ balls are disjoint.



$\lambda_1(L) \leq O_\varepsilon(1)$ $\Rightarrow$ at least $2^{-\varepsilon n}$ fraction of each ball overlaps.

Thanks for listening
(from all of us)!


Divesh Aggarwal


Huck Bennett


Zvika Brakerski


Sasha Golovnev


Rajendra Kumar


Zeyong Li


Spencer Peters


Noah Stephens-Davidowitz


Vinod Vaikuntanathan

I'm happy to take further questions at `sjpeters@cs.cornell.edu`.

Improved security guarantees

Prior work

- Private-key cryptography is secure if there are no polynomial-time algorithms for n-SVP.
- Public-key cryptography is secure if there are no poly-time *quantum* algorithms for $n^{1.5}$-SVP, OR if there are no poly-time *classical* algorithms for n^2-SVP.

This work

- Private-key cryptography is *exponentially* secure if there are no $2^{\varepsilon n}$-time algorithms for $\sqrt{n}$-SVP.
- Public-key cryptography is *exponentially* secure if there are no $2^{\varepsilon n}$-time algorithms for n-SVP.

Hardness Barriers

Prior work

- $\sqrt{n/\log n}$-SVP $\in$ coAM
- $\sqrt{n}$-SVP $\in$ coNP

Shows that $\sqrt{n/\log n}$-SVP is not NP-hard, assuming the polynomial hierarchy does not collapse.

This work

- $O_\varepsilon(1)$-SVP $\in \mathrm{coAMTime}[2^{\varepsilon n}]$
- $O_\varepsilon(\sqrt{\log n})$-SVP $\in \mathrm{coNTime}[2^{\varepsilon n}]$
- $O_\varepsilon(1)$-SVP $\in \mathrm{coMATime}[2^{\varepsilon n}]$
  - No analogue in poly-time world.

Shows that $O_\varepsilon(1)$-SVP is not exponentially hard, assuming variants of the Exponential Time Hypothesis.